PCT/JP03/09894

04.08.03

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　８月　５日

出願番号
Application Number: 特願２００２－２２７８８８

[ST. 10/C]: [ＪＰ２００２－２２７８８８]

出願人
Applicant(s): 財団法人大阪産業振興機構

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年　９月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７２２５１

【書類名】　特許願

【整理番号】　23526

【提出日】　平成14年 8月 5日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

【発明の名称】　データ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体

【請求項の数】　7

【発明者】

【住所又は居所】　大阪府茨木市美穂ヶ丘５番１号　大阪大学内

【氏名】　斉藤　和典

【特許出願人】

【識別番号】　801000061

【氏名又は名称】　財団法人大阪産業振興機構

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06(6944)4141

【選任した代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06(6944)4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

出証特２００３－３０７２２５１

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0117254

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体

【特許請求の範囲】

【請求項１】　複数の命令コードを含むデータの入力を受付け、受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、

分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とするデータ処理方法。

【請求項２】　複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項３】　前記命令コード群の復帰先アドレスに所定の文字列が対応付

けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくなしてあることを特徴とする請求項２に記載のデータ処理装置。

【請求項４】　複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出すための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項５】　複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出すための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項６】　コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、

コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判

断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有することを特徴とするコンピュータプログラム。

【請求項７】　コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、

コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とするコンピュータでの読取りが可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、不正な処理を実行するデータを検出するデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体に関する。

【０００２】

【従来の技術】

インターネット網の普及に伴い、各種の情報処理装置がコンピュータウィルス、クラッキング等の攻撃の対象となり、それらの脅威に晒される可能性が高くなってきている。

例えば、近年、「ニムダ」、「コードレッド」等のコンピュータウィルスに代表されるように、システムプログラム又はウェブブラウザのようなアプリケーションプログラムの脆弱性（セキュリティホール）を利用して自己増殖させ、甚大な被害を与えたケースが存在する。

【０００３】

前述のようなコンピュータウィルス、クラッキング等による攻撃では、不正な処理を行う命令コード（以下、不正コードという）を含む攻撃データを攻撃対象であるサーバ装置、パーソナルコンピュータ等の情報処理装置に対して送信し、その情報処理装置にて前記命令コードが実行されるようにしている。このような攻撃手法は様々なものが存在し、その１つとしてバッファオーバフローによる攻撃手法が知られている。バッファオーバフローでは、スタック内に確保されたバッファにおいて、確保されたバッファ以上のスタックエリアに書込みが行われている状態であり、バッファオーバフローの状態に陥った場合、予期せぬ変数破壊を招き、プログラムの誤動作の原因となり得る。バッファオーバフローによる攻撃では、プログラムの誤動作を意図的に引き起し、例えばシステムの管理者権限を取得することが行われる。

【０００４】

これらのコンピュータウィルス、クラッキング等の攻撃に対処するため、従来では、受信したデータに対して不正コードにみられる特定のビットパターンの有無を検出する。そして、そのようなビットパターンが受信したデータに含まれている場合には、不正コードを含んだ攻撃データであると判定し、データの受信拒否、ユーザへの報知等の処理を行うようにしている。

【０００５】

【発明が解決しようとする課題】

そのため、従来の手法により様々なコンピュータウィルス、クラッキング等の攻撃に対処するためには、各コンピュータウィルス、クラッキングに対応した特

定のビットパターンをデータベースに記憶させて予め用意しておく必要があり、新種のコンピュータウィルス、クラッキング手法が発見された場合には、前記データベースを更新して対処しなければならない。

【０００６】

ところで、攻撃データに対する従来の検出方法では、前述のように既知のビットパターンを検出するか、又はＮＯＰ命令（NOP：non-operation）の単純な繰り返しといった攻撃処理にとって、本質的とはいえない部分の構造を検出するようにしてきた。そのため、攻撃データのバリエーションに弱く、未知の攻撃データが現れる毎に、検出に用いるビットパターンのデータベースを更新する必要があり、データベースが更新されるまでのタイムラグが問題になっていた。

【０００７】

本発明は斯かる事情に鑑みてなされたものであり、分岐命令に係る命令コードを入力されたデータから検索し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する構成とすることにより、不正な処理を行う命令コード群を検出するためのビットパターンを予め用意する必要がなく、不正な処理を行う未知の命令コード群に対しても検出可能なデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】

第１発明に係るデータ処理方法は、複数の命令コードを含むデータの入力を受付け、受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記

憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とする。

【０００９】

第２発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【００１０】

第３発明に係るデータ処理装置は、第２発明に係るデータ処理装置において、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくなしてあることを特徴とする。

【００１１】

第４発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所

定の処理を実行する命令コード群を呼出すための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【００１２】

第５発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所定の処理を実行する命令コード群を呼出すための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【００１３】

第６発明に係るコンピュータプログラムは、コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有することを特徴とする。

【００１４】

第７発明に係るコンピュータでの読取りが可能な記録媒体は、コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とする。

【００１５】

第１発明、第２発明、第６発明、及び第７発明にあっては、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしている。したがって、通常のデータ（実行コード）には見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不正コードであるか否かの判定が可能であるため処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

【００１６】

第３発明にあっては、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

【００１７】

第４発明にあっては、所定の処理を実行する命令コード群を呼出すための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【００１８】

第５発明にあっては、所定の処理を実行する命令コード群を呼出すための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【００１９】

【発明の実施の形態】

以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

実施の形態１．

図１は本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図である。図中１０は本発明のデータ処理装置を具体化した中継装置であり、例えば、ルータ、スイッチ、ブロードバンドルータ等のデータ通信を中継する装置である。中継装置１０は、ＣＰＵ１１、メモリ１２、及び通信インターフェース（以下、通信ＩＦという）１３，１４を備えており、通信ＩＦ１３に接続された情報処理装置２０とインターネット網のようなデータ通信網Ｎを介して通信ＩＦ１４に接続された他の情報処理装置３０と間で、各種データの送受信を中継する。情報処理装置２０，３０は、例えば、パーソナルコンピュータ、サーバ装置、携帯電話機、ＰＤＡ（Personal Digital Asistant）等のデータ通信を行うことができる装置である。

情報処理装置３０から送信されたデータを中継装置１０が受信した際、中継装

置１０は受信したデータが不正な処理を実行する命令コード（以下、不正コードという）を含んだデータであるか否かを判断し、不正コードを含んでいる場合には、通信の遮断、警報の出力等の処理を行う。

【００２０】

中継装置１０のメモリ１２は、ルーティングテーブル１２ａ、フィルタリングテーブル１２ｂ、及び分岐テーブル１２ｃを備えている。

ルーティングテーブル１２ａには通信の経路制御情報が記憶されており、該経路制御情報によって、情報処理装置２０から送信されるデータの伝送経路が決定される。フィルタリングテーブル１２ｂには受信を拒否すべき通信相手の識別情報（例えば、ＩＰアドレス又はポート番号等）が記憶されており、前記識別情報に該当する情報処理装置からのデータを受信した場合、そのデータを情報処理装置２０へ送信しないようにしている。

また、メモリ１２には本発明のコンピュータプログラムが予め記憶されており、ＣＰＵ１１が当該コンピュータプログラムを実行することによって、中継装置１０は、不正コードを検出する侵入検出システムとして動作する。分岐テーブル１２ｃには、前記コンピュータプログラムが起動中に取得した特定の命令コードに係るメモリアドレス（以下、単にアドレスという）が記憶され、不正コードを含んだデータであるか否かを判断する際に利用される。

中継装置１０のＣＰＵ１１は、これらのテーブルに対して適宜書込み処理、又は読込み処理を行い、通信制御を行うようにしている。

【００２１】

以下、発明者らの知見に基づいて見出された不正コードの特徴的構造について説明する。発明者らは不正コードの普遍的な特徴として、分岐命令（以下、ｊｍｐ命令という）により指定された分岐先に呼出命令（以下、ｃａｌｌ命令という）が設定されていること、そしてその呼出先がｊｍｐ命令とｃａｌｌ命令との間にあることを見出している。そして、ｃａｌｌ命令によって、スタックへ格納されたアドレス、すなわちｃａｌｌ命令の次のアドレスを呼出し先の命令コード群にて取得して、取得したアドレスを用いて起動したいコマンドを実行させるようにしている。

【００２２】

図２及び図３は、不正コードの特徴的構造を説明する概念図である。前述したように、処理を分岐させるためのｊｍｐ命令の分岐先に対応させてｃａｌｌ命令を設定している。すなわち、ｊｍｐ命令の分岐先アドレス（Ａ１０）にｃａｌｌ命令を対応させている。

そして、ｃａｌｌ命令の呼出し先に、外部コマンドを呼び出すための命令コード群（Ａ２～Ａ６）を対応付け、そのｃａｌｌ命令による呼出し先が、分岐元アドレス（Ａ１）と分岐先アドレス（Ａ１０）との間にくるように設定している。この命令コード群において、ｃａｌｌ命令によってスタックへ格納されたアドレス、すなわちｃａｌｌ命令の次のアドレス（Ａ１１）をｐｏｐ命令によって取得し、取得したアドレスを利用して、外部コマンドを実行させるようにしている。

したがって、不正コードの作成者が意図した任意の外部コマンドをｃａｌｌ命令の次のアドレスに対応させることによって、これらの命令コードが実行されるときに、前記外部コマンドが呼出されて実行される構成となっている。

なお、前記命令コード群とｃａｌｌ命令との間（Ａ７～Ａ９）にはダミーの初期データ及び作業領域を設けても良いことは勿論である。

【００２３】

前述した不正コードは、図３に模式的に示した如く、（１）ｊｍｐ命令の分岐先にｃａｌｌ命令が存在すること、（２）ｃａｌｌ命令の呼出先がｃａｌｌ命令とｊｍｐ命令との間に存在することを特徴としている。

中継装置１０では、このような特徴的構造を持つ不正コードを通信ＩＦ１４にて受信したデータから検出し、警報を出力するか又は通信の遮断を行うようにしている。

【００２４】

以下、前述した特徴的構造をもつ不正コードの検出手順について説明する。図４は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートであり、図５は侵入検出の際に利用される分岐テーブル１２ｃの一例を示す概念図である。まず、中継装置１０のＣＰＵ１１は通信ＩＦ１４にて受信したデータを１バイト読込む（ステップＳ１）。そして、ＣＰＵ１１は、読込んだデータが

ｊｍｐ命令か否かを判断する（ステップＳ２）。読込んだデータがｊｍｐ命令である場合（Ｓ２：ＹＥＳ）、ＣＰＵ１１は、そのｊｍｐ命令で指定される分岐先のアドレスが、現在位置のアドレスよりも大きいか否かを判断する（ステップＳ３）。

【００２５】

分岐先のアドレスが現在位置のアドレスよりも大きいと判断した場合（Ｓ３：ＹＥＳ）、現在位置のアドレス（分岐元アドレス）と分岐先のアドレス（分岐先アドレス）とを対応付けて分岐テーブル１２ｃに記憶させる（ステップＳ４）。図２に示した如きデータの例では、アドレスＡ１のデータを読込んだ場合、そのデータはｊｍｐ命令であり、当該ｊｍｐ命令で指定される分岐先のアドレス（Ａ１０）がアドレスＡ１よりも大きいため、分岐元アドレスとしてＡ１、分岐先アドレスとしてＡ１０が分岐テーブル１２ｃに記憶される（図５参照）。

【００２６】

ステップＳ３にて、分岐先アドレスが現在位置のアドレスよりも小さいと判断した場合（Ｓ３：ＮＯ）、又はステップＳ４にて、分岐テーブル１２ｃに分岐元アドレスと分岐先アドレスとを記憶させた場合、ＣＰＵ１１は、読込むべきデータが終了したか否かを判断し（ステップＳ５）、読込むべきデータが未だ残っていると判断した場合（Ｓ５：ＮＯ）、処理をステップＳ１へ戻し、読込むべきデータが終了したと判断した場合（Ｓ５：ＹＥＳ）、本ルーチンを終了する。

【００２７】

ステップＳ２において、読込んだデータｊｍｐ命令でないと判断した場合（Ｓ２：ＮＯ）、ＣＰＵ１１は、現在位置のアドレスが分岐テーブル１２ｃに記憶された分岐先アドレスに一致するか否かを判断する（ステップＳ６）。現在位置のアドレスが分岐先のアドレスに一致しない場合（Ｓ６：ＮＯ）、現在位置のアドレスより小さい分岐先アドレスを分岐テーブル１２ｃから削除する（ステップＳ７）。そして、ステップＳ５の処理を行い、再度ステップＳ１へ処理を戻すか、又は本ルーチンの処理を終了するか否かの判断をする。

【００２８】

現在位置のアドレスが分岐テーブル１２ｃに記憶された分岐先アドレスに一致

すると判断した場合（Ｓ６：ＹＥＳ）、ＣＰＵ１１は、現在位置のアドレスに対応付けられた命令コードがｃａｌｌ命令であるか否かを判断する（ステップＳ８）。現在位置のアドレスに対応付けられた命令コードがｃａｌｌ命令であると判断した場合（Ｓ８：ＹＥＳ）、ＣＰＵ１１は、分岐テーブル１２ｃを参照することによって、前記ｃａｌｌ命令による呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断する（ステップＳ９）。

ステップＳ８にて、ｃａｌｌ命令でないと判断した場合（Ｓ８：ＮＯ）、又はステップＳ９にて、呼出先が分岐元アドレスと分岐先アドレスとの間にないと判断した場合（Ｓ９：ＮＯ）、処理をステップＳ５へ移行させる。

【００２９】

ｃａｌｌ命令による呼出先が分岐テーブル１２ｃに記憶された分岐元アドレスと分岐先アドレスとの間にあると判断した場合（Ｓ９：ＹＥＳ）、ＣＰＵ１１は、不正コードを検出した旨の情報を生成する（ステップＳ１０）。

【００３０】

前述の不正コードを検出した旨の情報は、中継装置１０に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、ＬＥＤランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置２０へ送信し、情報処理装置２０が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて通信を遮断するようにしてもよい。

【００３１】

なお、前述したようにｃａｌｌ命令によりスタックへ格納されるアドレスには、実行させたい外部コマンドの文字列が存在するため、ｃａｌｌ命令の次のアドレスにアスキー文字列（コマンド名）が存在するか否かを傍証として利用することにより、不正コードの検出精度を向上させることができる。

また、ｃａｌｌ命令の次のアドレスにアスキー文字列が存在するか否かについての判断を単独で行うことによっても、不正コードの有無を検出できることが発明者らの検討により知られている。

【００３２】

このように、本実施の形態では、データを逐次的に読込んで処理することにより、不正コードが含まれているか否かについて判断できるため、不正コードの有無を検出するアルゴリズムが簡単であり、しかも高速処理が可能である。

【００３３】

実施の形態２．

前述の不正コードでは、ｃａｌｌ命令の次のアドレスに実行させたい外部コマンドを置くこと特徴としており、実施の形態１では、そのような外部コマンドを呼出すための特殊な構造を見出すことによって、不正コードを検出していた。しかしながら、実行させたい外部コマンドは必ずしもｃａｌｌ命令の次に置く必要はなく、不正コードの作者によって予め定められたアドレス分だけ位置をずらして置くことも可能である。このような不正コードをここでは偽装された不正コードと呼び、以下、この偽装された不正コードの特徴的構造、及び検出手順について説明する。なお、中継装置１０の構成、及び情報処理装置２０，３０との接続構成は実施の形態１と同様であるため説明を省略する。

【００３４】

図６及び図７は偽装された不正コードの特徴的構造を説明する概念図である。偽装された不正コードでも、ｃａｌｌ命令によって呼出された命令コード群において、起動したい外部コマンドに対応付けられているアドレスを取得するようにしていることは前述と同様であるが、ｃａｌｌ命令と外部コマンドとの間に固定長を有するダミーの命令コードを置いて偽装していることが実施の形態１で説明した不正コードと異なる。

すなわち、図６に示した構造を有する偽装された不正コードでは、ｃａｌｌ命令によりスタックへ格納されたアドレス（Ａ２）を、Ａ１６～Ａ２０に規定された命令コード群にて取得し、そのアドレスＡ２から５つ目のアドレス（Ａ７）に対応付けられている外部コマンドを起動させるようにするのである。

【００３５】

このような偽装された不正コードは、実施の形態１で説明した処理によっては検出不可能であるが、図７に模式的に示した如く、（１）ｃａｌｌ命令によって命令コード群を呼出し、（２）その命令コード群において、ｃａｌｌ命令によっ

てスタックへ格納したアドレスをｐｏｐ命令により取得するという特徴的構造を依然として有していることが分かる。したがって、ｃａｌｌ命令によって呼出された命令コード群において、ｐｕｓｈ命令が先行しないｐｏｐ命令を検索することによって、偽装された不正コードを検出することが可能となる。

【００３６】

以下、偽装された不正コードの検出手順について説明する。

図８は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。まず、中継装置１０のＣＰＵ１１は、受信したデータからｃａｌｌ命令を検索する（ステップＳ２１）。そして、検索の結果、ｃａｌｌ命令があるか否かを判断し（ステップＳ２２）、ｃａｌｌ命令がある場合（Ｓ２２：ＹＥＳ）、ＣＰＵ１１は、検索されたｃａｌｌ命令のアドレスをメモリ１２に記憶させる（ステップＳ２３）。受信したデータにｃａｌｌ命令がない場合（Ｓ２２：ＮＯ）、本侵入検出システムによる処理を終了する。

【００３７】

検索されたｃａｌｌ命令のアドレスを記憶させた後、そのｃａｌｌ命令により指定される呼出先アドレスへ移動させ（ステップＳ２４）、データを１バイト読込む（ステップＳ２５）。

次いで、ＣＰＵ１１は、読込んだデータがスタックへアドレスを格納するためのｐｕｓｈ命令か否かを判断する（ステップＳ２６）。ｐｕｓｈ命令であると判断した場合（Ｓ２６：ＹＥＳ）、現在アドレスを記憶して（ステップＳ２７）、処理をステップＳ２５へ戻す。

【００３８】

読込んだデータがｐｕｓｈ命令でないと判断した場合（Ｓ２６：ＮＯ）、ｐｏｐ命令であるか否かを判断する（ステップＳ２８）。ｐｏｐ命令でないと判断した場合（Ｓ２８：ＮＯ）、呼出先のルーチンが終了したか否かを判断する（ステップＳ３１）。

呼出先のルーチンが終了していないと判断した場合（Ｓ３１：ＮＯ）、処理をステップＳ２５へ戻し、呼出先のルーチンが終了したと判断した場合（Ｓ３１：ＹＥＳ）、ステップＳ２３にて記憶させたアドレスを参照し、呼出元の次のアド

レスへ移動させ（ステップＳ３２）、ｃａｌｌ命令を再度検索し直す。

【００３９】

ステップＳ２５で読込んだデータがｐｏｐ命令であると判断した場合（Ｓ２８：ＹＥＳ）、ＣＰＵ１１は、ステップＳ２７にて記憶させたアドレスを参照することによって、ｐｕｓｈ命令が先行しないｐｏｐ命令であるか否かを判断する（ステップＳ２９）。ｐｕｓｈ命令が先行しないｐｏｐ命令でないと判断した場合（Ｓ２９：ＮＯ）、処理をステップＳ３１へ移行する。

【００４０】

ステップＳ２５で読込んだデータが、ｐｕｓｈ命令が先行しないｐｏｐ命令であると判断した場合（Ｓ２９：ＹＥＳ）、ＣＰＵ１１は、不正コードを検出した旨の情報を生成する（ステップＳ３０）。

【００４１】

前述の不正コードを検出した旨の情報は、実施の形態１と同様に、中継装置１０に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、ＬＥＤランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置２０へ送信し、情報処理装置２０が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて通信を遮断するようにしてもよい。

【００４２】

実施の形態３．

前述の実施の形態では、ルータ、スイッチ、ブロードバンドルータ等のデータ通信で利用される中継装置に本発明を適用した形態について説明したが、パーソナルコンピュータ、サーバ装置、携帯電話機、ＰＤＡ等の通信機能を有した情報処理装置に適用することも可能である。

【００４３】

図９は本実施の形態に係る侵入検知システムの構成を説明する模式図である。図中５０は、パーソナルコンピュータのような情報処理装置であり、該情報処理装置５０にはルータのような中継装置４０を介してデータ通信網Ｎへ接続されている。情報処理装置５０は、データ通信網Ｎ及び中継装置４０を通じて各種の通

信機器、及び他の情報処理装置からデータを受信するとともに、それらの通信機器、情報処理装置へデータを送信するようにしている。

【００４４】

中継装置４０には、ＣＰＵ４１、メモリ４２、及び通信ＩＦ４３、４４を備えており、メモリ４２には、通信の経路制御情報が記憶されたルーティングテーブル４２ａと、受信を拒否すべき通信相手の識別情報（例えば、ＩＰアドレス又はポート番号等）が記憶されたフィルタリングテーブル４２ｂとを有している。情報処理装置５０から外部へデータを送信する際にルーティングテーブル４２ａにより伝送経路が設定され、外部からデータを受信する際、フィルタリングテーブル４２ｂを参照することにより受信を拒否すべき通信相手であるか否かが判定される。

【００４５】

情報処理装置５０は、ＣＰＵ５１を備えており、バス５２を介して、ＲＯＭ５３、ＲＡＭ５４、表示部５５、入力部５６、通信部５７、補助記憶装置５８、及び内部記憶装置５９等の各種ハードウェアに接続されている。ＣＰＵ５１は、ＲＯＭ５３に格納された制御プログラムに従って、それらのハードウェアを制御する。ＲＡＭ５４は、ＳＲＡＭ又はフラッシュメモリ等で構成され、ＲＯＭ５３に格納された制御プログラムの実行時に発生するデータを記憶する。

【００４６】

表示部５５は、ＣＲＴ、液晶ディスプレイ等の表示装置であり、入力部５６は、キーボード、マウス等の入力装置である。表示部５５及び入力部５６は、例えば、送信すべきデータの入力及び表示をする際に利用される。通信部５７は、モデム等の回線終端装置を備えており、中継装置４０を介した各種データの送受信を制御する。

【００４７】

補助記憶装置５８は、本発明のコンピュータプログラム及びデータを記録したＦＤ、ＣＤ－ＲＯＭ等の記録媒体６０からコンピュータプログラム及びデータを読取るＦＤドライブ、ＣＤ－ＲＯＭドライブ等からなり、読取られたコンピュータプログラム及びデータは、内部記憶装置５９に記憶される。内部記憶装置５９

に記憶されているコンピュータプログラム及びデータは、ＲＡＭ５４に読込まれ、ＣＰＵ５１が実行することで本実施の形態に係る情報処理装置５０として動作する。

なお、本発明のコンピュータプログラムは、記録媒体６０により提供されるだけでなく、データ通信網Ｎを通じて提供される形態であってもよいことは勿論である。

【００４８】

前述のコンピュータプログラムは、情報処理装置５０の起動時に自動的にＲＡＭ５４に読込まれる常駐型のプログラムであることが望ましく、通信部５７にて外部からデータを受信した際に、自動的に不正コードを検出するようにしておくとよい。なお、不正コードの検出手順については、実施の形態１及び実施の形態２で説明した通りであるので説明を省略する。

【００４９】

本実施の形態では、パーソナルコンピュータのような情報処理装置５０を利用して不正コードを含んだデータを検出する構成としたが、パーソナルコンピュータの他、携帯電話機、ＰＤＡ、コンピュータゲーム機、車載通信装置、各種の情報家電に適用できることは勿論である。

また、本発明のコンピュータプログラムをＦＤ、ＣＤ－ＲＯＭ等の記録媒体に記録させて提供することにより、コンピュータウィルスを検出するアプリケーションソフトウェアのパッケージとして提供することも可能である。

【００５０】

【発明の効果】

以上、詳述したように、第１発明、第２発明、第６発明、及び第７発明による場合は、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしてい

る。したがって、通常の実行コードでは見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不正コードであるか否かの判定が可能であるため処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

【００５１】

第３発明による場合は、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

【００５２】

第４発明に場合は、所定の処理を実行する命令コード群を呼出すための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【００５３】

第５発明による場合は、所定の処理を実行する命令コード群を呼出すための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる等、本発明は優れた効果を奏する。

【図面の簡単な説明】

【図１】

本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図である。

【図２】

不正コードの特徴的構造を説明する概念図である。

【図３】

不正コードの特徴的構造を説明する概念図である。

【図４】

本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。

【図５】

侵入検出の際に利用される分岐テーブルの一例を示す概念図である。

【図６】

偽装された不正コードの特徴的構造を説明する概念図である。

【図７】

偽装された不正コードの特徴的構造を説明する概念図である。

【図８】

本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。

【図９】

本実施の形態に係る侵入検知システムの構成を説明する模式図である。

【符号の説明】

１０　中継装置

１１　ＣＰＵ

１２　メモリ

１２ａ　ルーティングテーブル

１２ｂ　フィルタリングテーブル

１２ｃ　分岐テーブル

１３　通信ＩＦ

１４　通信ＩＦ

２０　情報処理装置

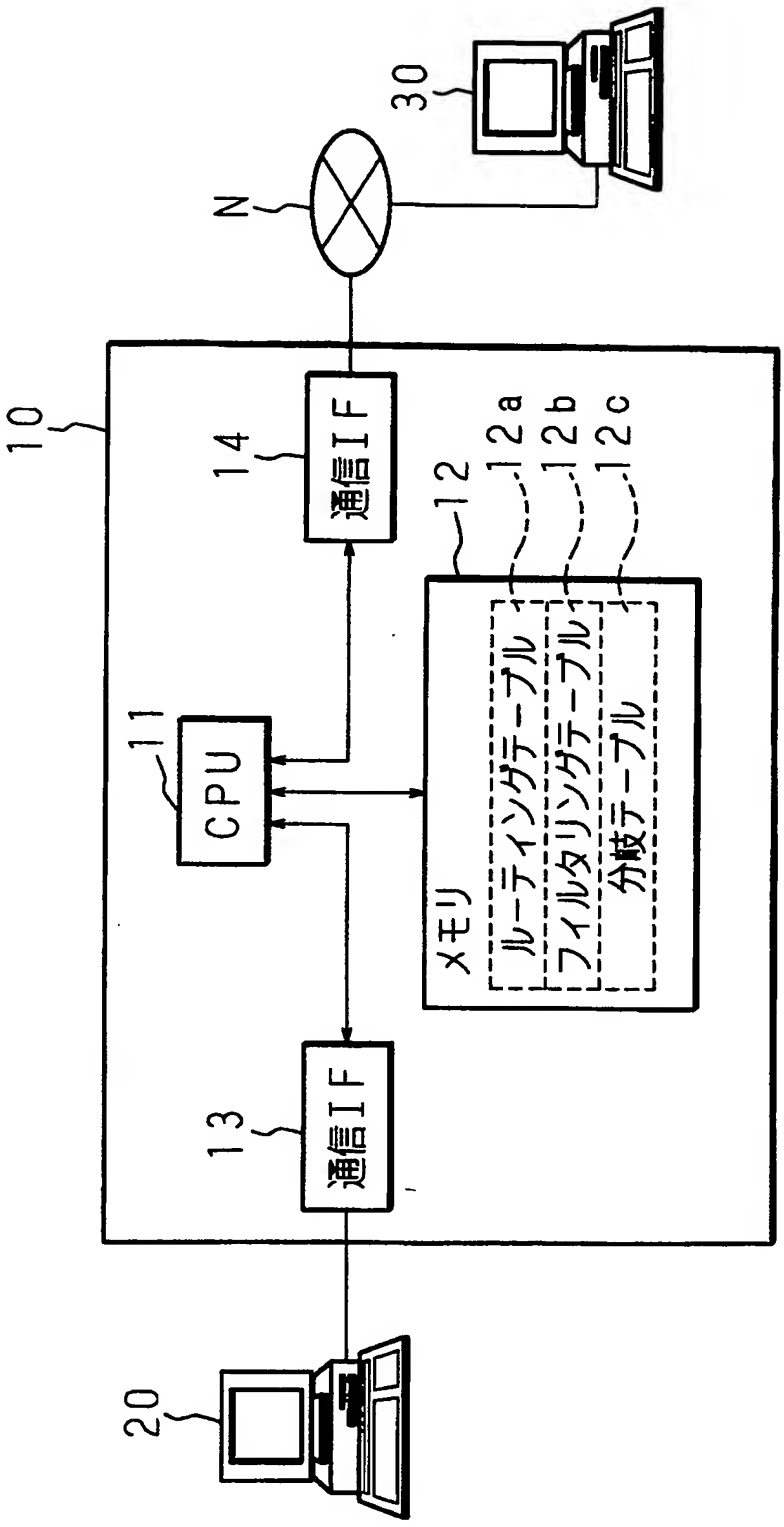
３０　情報処理装置

５０　情報処理装置

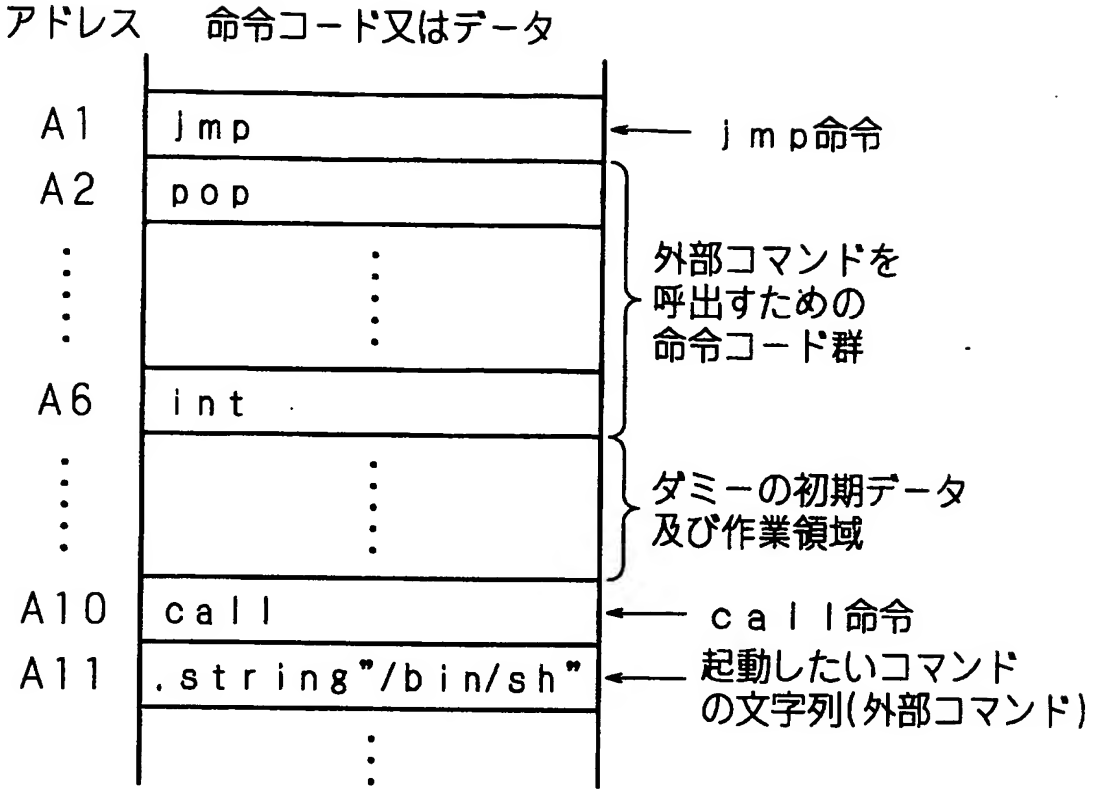
Ｎ　データ通信網

【書類名】　　図面

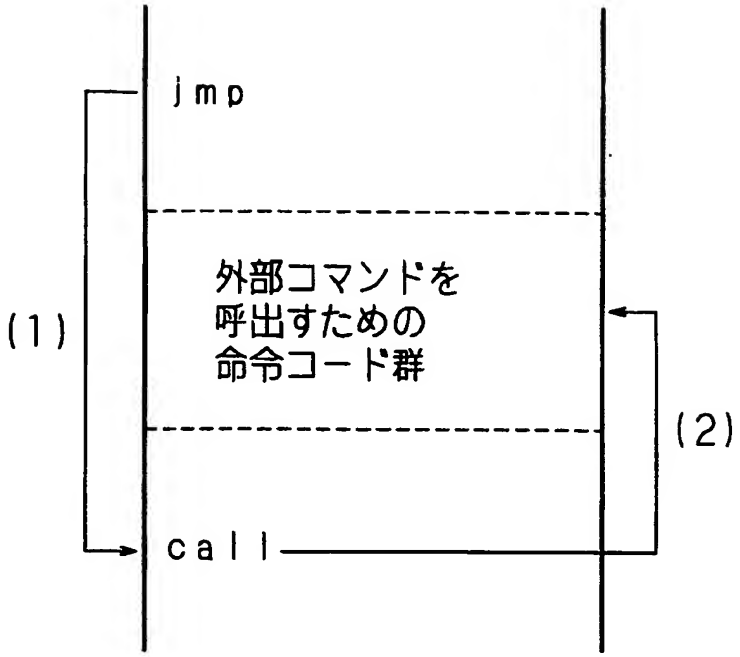
【図１】


30
N
10
14
通信IF
12
12a
12b
12c
メモリ
ルーティングテーブル
フィルタリングテーブル
分岐テーブル
11
CPU
13
通信IF
20

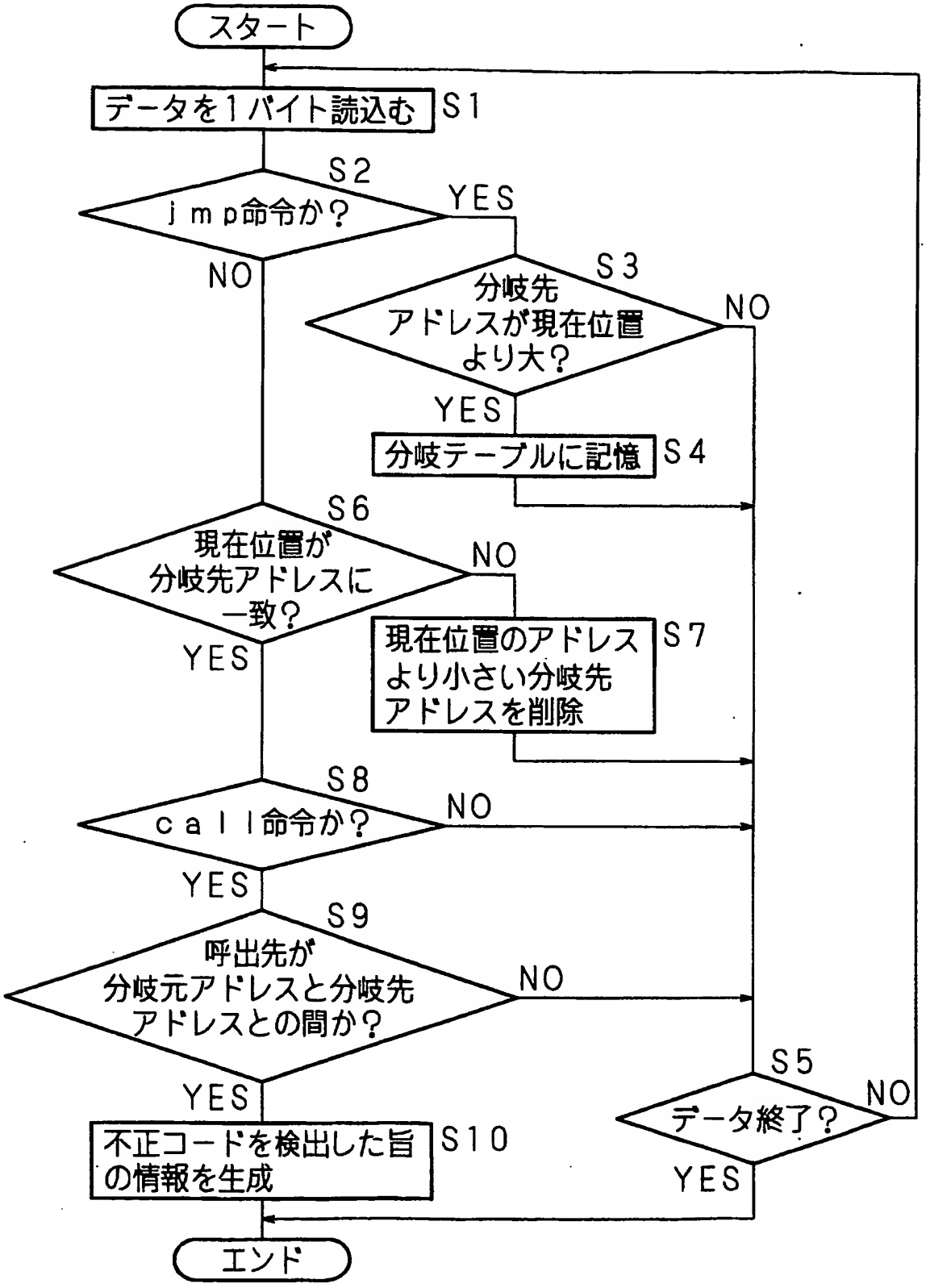
【図２】


アドレス
命令コード又はデータ
A1
jmp
A2
pop
A6
int
A10
call
A11
.string"/bin/sh"
jmp命令
外部コマンドを
呼出すための
命令コード群
ダミーの初期データ
及び作業領域
call命令
起動したいコマンド
の文字列(外部コマンド)

【図３】



【図４】

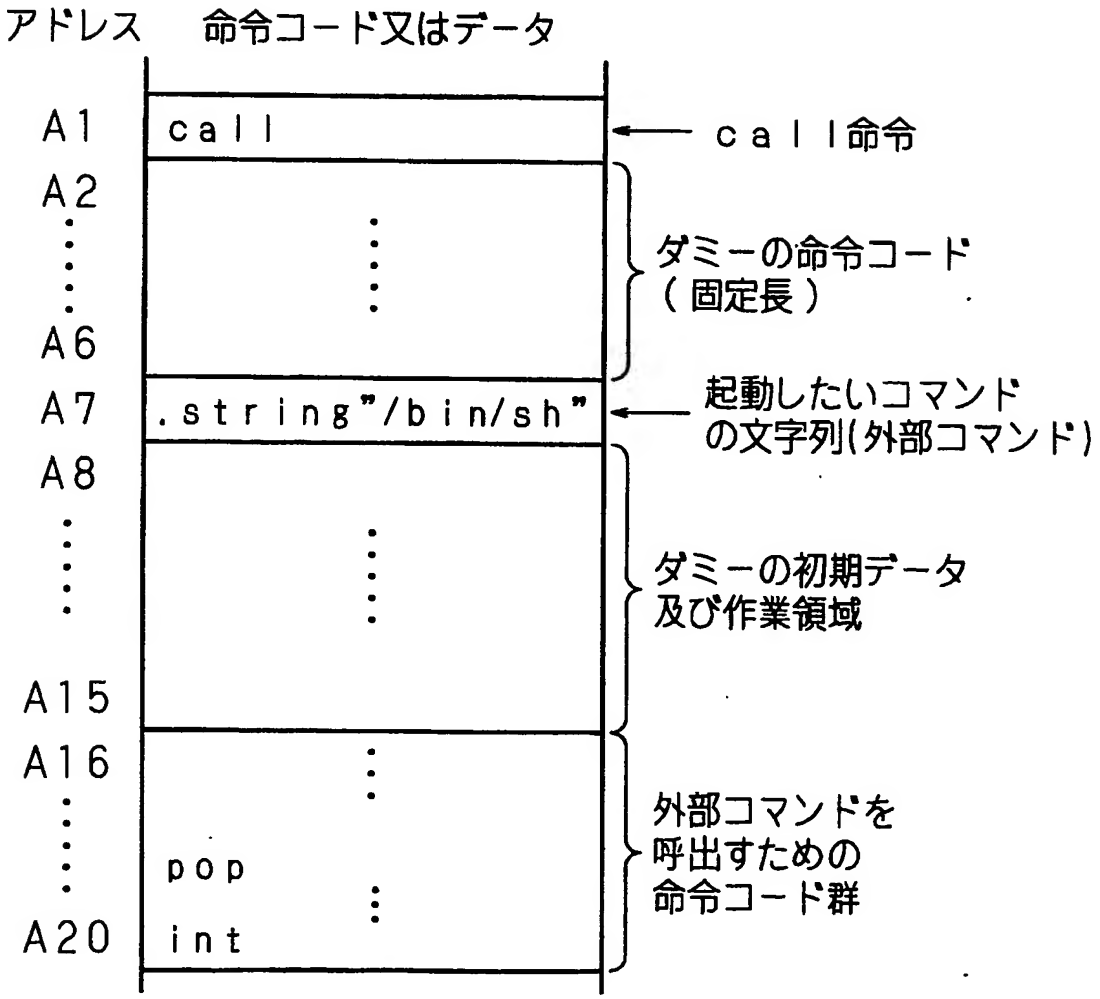

スタート
データを１バイト読込む
S1
S2
ｊｍｐ命令か？
YES
NO
S3
分岐先
アドレスが現在位置
より大？
NO
YES
分岐テーブルに記憶
S4
S6
現在位置が
分岐先アドレスに
一致？
NO
YES
現在位置のアドレス
より小さい分岐先
アドレスを削除
S7
S8
ｃａｌｌ命令か？
NO
YES
S9
呼出先が
分岐元アドレスと分岐先
アドレスとの間か？
NO
YES
S5
データ終了？
NO
YES
不正コードを検出した旨
の情報を生成
S10
エンド

【図５】

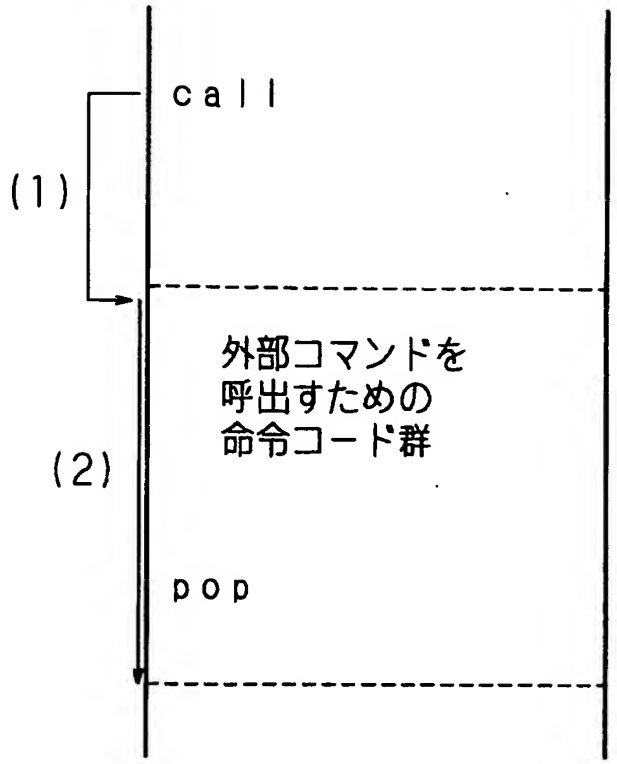
12c

分岐元アドレス	分岐先アドレス
A1	A10
⋮	⋮

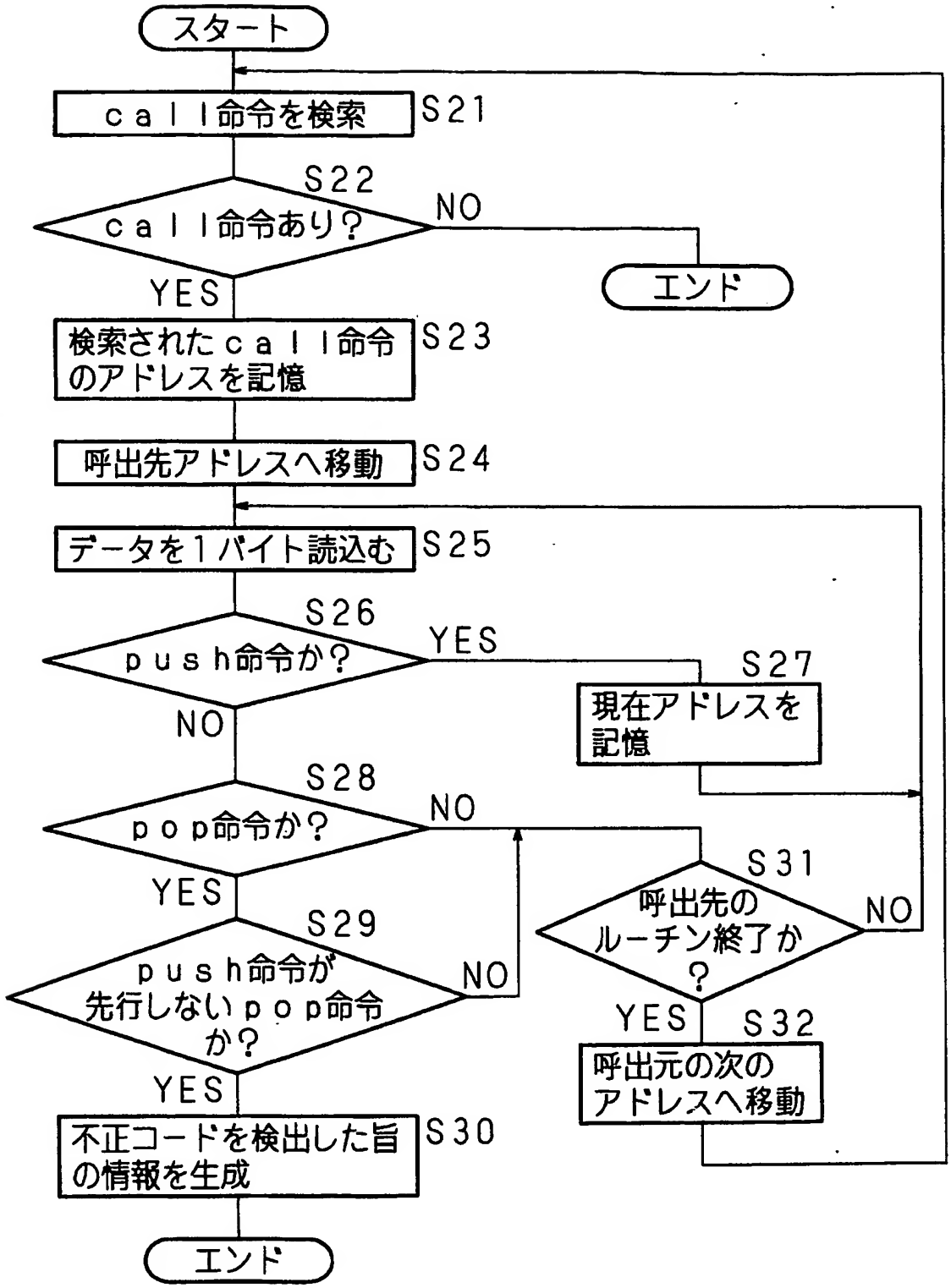
【図６】



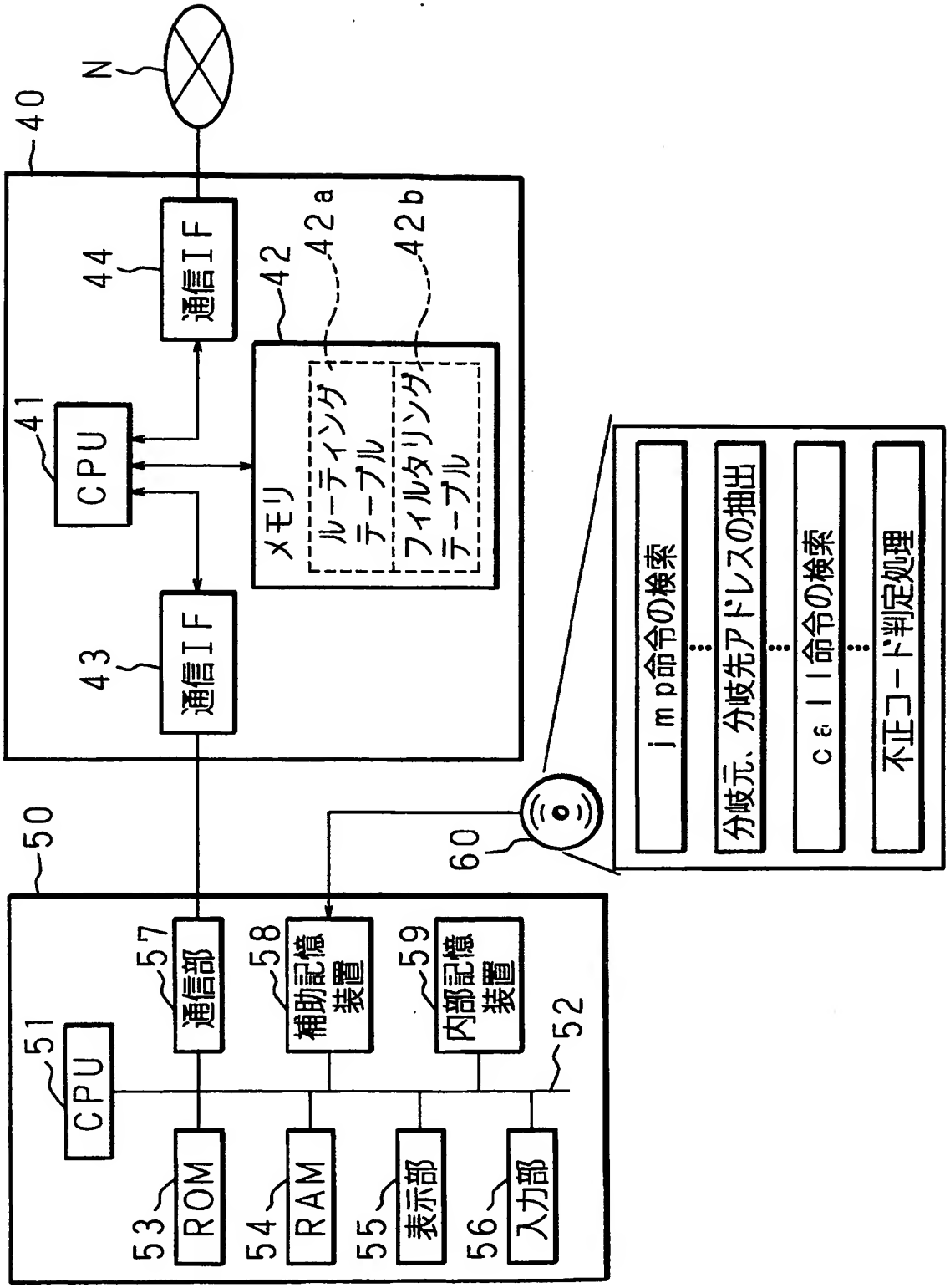
【図７】



【図８】


スタート
ｃａｌｌ命令を検索
S21
S22
ｃａｌｌ命令あり？
NO
エンド
YES
検索されたｃａｌｌ命令のアドレスを記憶
S23
呼出先アドレスへ移動
S24
データを１バイト読込む
S25
S26
ｐｕｓｈ命令か？
YES
S27
現在アドレスを記憶
NO
S28
ｐｏｐ命令か？
NO
S31
呼出先のルーチン終了か？
NO
YES
S29
ｐｕｓｈ命令が先行しないｐｏｐ命令か？
NO
YES
S32
呼出元の次のアドレスへ移動
YES
不正コードを検出した旨の情報を生成
S30
エンド

【図９】


N
40
通信ＩＦ
44
42
42a
42b
CPU
41
メモリ
ルーティングテーブル
フィルタリングテーブル
通信ＩＦ
43
50
60
jmp命令の検索
分岐元、分岐先アドレスの抽出
call命令の検索
不正コード判定処理
CPU
51
通信部
57
補助記憶装置
58
内部記憶装置
59
52
ROM
53
RAM
54
表示部
55
入力部
56

【書類名】　要約書

【要約】

【課題】　不正コードの本質的構造を見抜いて検出することができるデータ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体の提供。

【解決手段】　分岐命令（ｊｍｐ命令）の分岐元アドレスと分岐先アドレスとを記憶し（Ｓ４）、分岐先アドレスに外部コマンドを実行させるための命令コード群を呼出すための呼出命令（ｃａｌｌ命令）が対応付けられているか否かを判断し（Ｓ６）、呼出命令が分岐先アドレスに対応付けられている場合、その呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断し（Ｓ９）、呼出命令による呼出先が分岐元アドレスと分岐先アドレスとの間にある場合、不正コードを検出した旨の情報を生成する（Ｓ１０）。

【選択図】　図４

特願２００２－２２７８８８

出　願　人　履　歴　情　報

識別番号　　［８０１０００００６１］

１．変更年月日　　２００１年　９月１３日
［変更理由］　　新規登録
住　所　　大阪府大阪市中央区本町橋２番５号　マイドームおおさか内
氏　名　　財団法人大阪産業振興機構